RFC-2350

The following profile of CERT-Bundesbank has been composed according to RFC-2350. This document describes organizational and technical interfaces and how to contact CERT-Bundesbank, the Computer Security Incident Response Team of Deutsche Bundesbank.

1 Document Information

1.1 Date of Last Update

Version 1.01, updated on 05.03.2019

1.2 Distribution List for Notifications

There is no distribution list for notifications.

1.3 Locations where this Document May Be Found

The current version of this document is available from the CERT-Bundesbank website at https://www.bundesbank.de/cert

1.4 Authenticating this Document

This document can be retrieved from our webserver using TLS/SSL.

2 Contact Information

2.1 Name of the Team

CERT Deutsche Bundesbank: CERT-Bundesbank

2.2 Address

Deutsche Bundesbank
CERT-Bundesbank
Wilhelm-Epstein-Straße 14
60431 Frankfurt am Main

2.3 Time Zone

Central European Time / Central European Summer Time
UTC+1 / UTC+2

2.4 Telephone Number

+49 69 9566 2925

2.5 Facsimile Number

+49 69 9566 50 9815

2.6 Other Telecommunications

None

2.7 Electronic Mail Address

If you need to notify us about an information security incident or a cyber-threat targeting or involving Deutsche Bundesbank, please contact us at:
CERT@bundesbank.de

2.8 Public Keys and Encryption Information

CERT-Bundesbank has a public PGP key which is available at:
https://www.bundesbank.de/en/service/banks-and-companies/pki/pgp
The S/MIME domain key is available at:
https://www.bundesbank.de/en/service/banks-and-companies/pki/user-certificates-621010

2.9 Team Members

No information is provided in public.

2.10 Other Information

General information about CERT-Bundesbank can be found at:
https://www.bundesbank.de/cert

2.11 Points of Customer Contact

The preferred method for contacting CERT-Bundesbank is via e-mail at
CERT@bundesbank.de
Please use PGP or S/MIME if you intend to send sensitive information.
The CERT-Bundesbank hours of operation are restricted to regular business hours from Monday to Friday, except public holidays in Germany/Hesse).
Urgent cases can be reported by phone (+49 69 9566 2925) 24/7.

3 Charter

3.1 Mission Statement

The purpose of CERT-Bundesbank is to promptly detect anomalies, attacks from internal and external sources and other security incidents concerning the security relevant IT infrastructure and applications of Deutsche Bundesbank. The activities cover prediction, prevention, detection and response. CERT-Bundesbank can initiate the appropriate countermeasures autonomously. Another goal is to support various internal departments to enhance the security level through vulnerability and penetration testing.

3.2 Constituency

The CERT-Bundesbank's constituency are the people and IT-assets (systems, networks and applications) of Deutsche Bundesbank.

3.3 Sponsorship and/or Affiliation

CERT-Bundesbank is affiliated to Deutsche Bundesbank.

3.4 Authority

The CERT-Bundesbank operates under the auspices of and with authority delegated by Director General of the Information Technology Department of Deutsche Bundesbank.

4 Policies

4.1 Types of Incidents and Level of Support

The CERT-Bundesbank is authorized to address all types of computer security incidents which occur, or threaten to occur, at Deutsche Bundesbank.
The level of support given by CERT-Bundesbank will vary depending on the severity of the security incident or issue, its potential or assessed impact and available CERT-Bundesbank's resources at the time.

4.2 Co-operation, Interaction and Disclosure of Information

CERT-Bundesbank operates within the current German, ESCB and general European legal frameworks, specifically regarding the handling and disclosure of information.
Co-operation with other CERTs or CSIRTs is regarded as a key task of operating as CERT. In scope of such a co-operation, CERT-Bundesbank will share information only if the protection of the identity of members of the constituency and of neighbouring sites where necessary, is given.

4.3 Communication and Authentication

The preferred method of communication with CERT-Bundesbank is e-mail.
For information about PGP and S/MIME keys please refer to sections 2.8 and 2.11.

5 Services

5.1 Incident Response

CERT-Bundesbank maintains the following incident response services for its constituency:

- Incident Analysis
- Incident Response Support
- Incident Response Coordination

5.2 Announcements

CERT-Bundesbank maintains “Announcements” as a proactive service for its constituency.

5.3 Alerts and Warnings

CERT-Bundesbank maintains “Alerts and Warnings” as an additional reactive service, which interacts with the proactive “Announcements” service.

6. Incident Reporting Forms

No special form is needed to report incidents to CERT-Bundesbank.
In case of emergency or crisis, please provide CERT-Bundesbank at least the following information:

- contact details and organizational information – name of person and organization name and address
- e-mail address, telephone number
- IP address(es), FQDN(s), and any other relevant technical elements with associated observation
- a relevant extract from the log showing the problem
- in case of forwarding e-mails to CERT-Bundesbank, please include all e-mail headers, body and any attachments if possible and as permitted by the regulations, policies and legislation under which you operate

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, CERT-Bundesbank assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.